

Резервное копирование и восстановление KUMA

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/222208.htm>

Резервное копирование и восстановление KUMA версии 2.1+

В связи с появлением возможности организации отказоустойчивого ядра в кластере kubernetes добавился новый механизм создания резервных копий ядра. Данный механизм использует API системы и в дальнейшем будет основным механизмом резервного копирования и восстановления.

Создание резервной копии Ядра KUMA по API

Для создания **резервной копии ресурсов и сертификатов** необходимо отправить следующий API-запрос:

GET /api/v1/system/backup

В ответ на запрос возвращается архив tar.gz, содержащий резервную копию Ядра KUMA. На хосте, где установлено Ядро, резервная копия не сохраняется. Сертификаты включаются в состав резервной копии.

Если операция выполнена успешно, создается событие аудита со следующими параметрами:

DeviceAction = "Core backup created"

SourceUserID = "<user-login>"

Пример команды для бэкапа через curl:

```
curl -k --header 'Authorization: Bearer <token>' 'https://<ip_kuma>:7223/api/v1/system/backup' -o backup.tar.gz
```

У токена пользователя должны быть соответствующие права для выполнения бекапа

Восстановление Ядра KUMA из резервной копии по API

Восстановление данных из резервной копии доступно только при сохранении версии KUMA.

Необходим работающий сервис MongoDB.

Если сервис MongoDB в нерабочем состоянии

Останавливаете службы MongoDB и Core:

```
systemctl stop kuma-mongodb.service  
systemctl stop kuma-core*.service
```

Удаляете данные из папки data:

```
rm -rf /opt/kaspersky/kuma/mongodb/data/*
```

Запускаете службу MongoDB:

```
systemctl start kuma-mongodb.service
```

Инициализируете MongoDB:

```
/opt/kaspersky/kuma/mongodb/bin/mongo --eval 'rs.initiate()'
```

Запускаете службу Core:

```
systemctl start kuma-core*.service
```

Далее восстанавливаете ядро по пунктам ниже этой главы.

Для восстановления из резервной копии необходимо отправить следующий API-запрос:

POST /api/v1/system/restore

```
curl -k --request POST 'https://<ip_kuma>:7223/api/v1/system/restore' --header 'Authorization: Bearer <token>' --data-binary '@/backup/backup.tar.gz'
```

Тело запроса должно содержать архив с резервной копией Ядра KUMA, полученный в результате выполнения API-запроса создания резервной копии.

После получения архива с резервной копией KUMA выполняет следующие действия:

1. Распаковывает архив с резервной копией Ядра KUMA во временную директорию.
2. Сравнивает версию текущей KUMA и с версией резервной копии KUMA.
3. Если версии соответствуют друг другу, создается событие аудита со следующими параметрами:

DeviceAction = "Core restore scheduled"

SourceUserID = "<имя пользователя инициировавшего восстановление KUMA из резервной копии"

4. Если версии не различаются, выполняет восстановление данных из резервной копии Ядра KUMA.

5. Удаляет временную директорию и запускает в штатном режиме.

В журнале Ядра KUMA появится запись "WARN: restored from backup".

Резервное копирование и восстановление KUMA до версии 2.1 (включительно)

Для создания резервной **копии баз ресурсов и сертификатов** можно использовать команду:

```
sudo /opt/kaspersky/kuma/kuma tools backup --dst <путь к директории для резервной копии> --certificates
```

Для создания резервной копии баз можно использовать команду:

```
sudo /opt/kaspersky/kuma/kuma tools backup --dst <путь к директории для резервной копии>
```

(Best Practice) Для автоматизации создания еженедельной (каждое воскресенье в 00:00) резервной копии (в защищенном виде, файлы будут находиться в папке /root/backup/ его можно заменить по желанию) создайте задачу в планировщике CRON следующей командой (выполняется от суперпользователя и в одну строку):

```
mkdir /root/backup ; echo PATH=$PATH >> /var/spool/cron/root ; echo SHELL=$SHELL >> /var/spool/cron/root ; echo "# m h dom mon dow user  command" >> /var/spool/cron/root ; echo "# m h dom mon dow user command" >> /var/spool/cron/root ; echo "0 0 * * 0 /opt/kaspersky/kuma/kuma tools backup --dst /root/backup/ --certificates" >> /var/spool/cron/root ; echo "#0 0 * * 0 /opt/kaspersky/kuma/kuma tools backup --dst /root/backup/" >> /var/spool/cron/root
```

Чтобы восстановить данные из резервной копии, войдите в ОС сервера, на котором установлено Ядро KUMA. Остановите Ядро KUMA, выполнив следующую команду:

```
sudo systemctl stop kuma-core
```

Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma tools restore --src <путь к директории с резервной копией> --certificates
```

Флаг --certificates не является обязательным и используется для восстановления сертификатов.

Запустите KUMA, выполнив следующую команду:

```
sudo systemctl start kuma-core
```

(опционально) Для создания незащищенной резервной копии конфигураций ресурсов KUMA можно использовать команду, файл сохраните на отдельном носителе (файл будет находиться в папке /home):

```
/opt/kaspersky/kuma/mongodb/bin/mongodump --db=kuma --archive=/home/kuma_dump_$(date +"%d%m%Y")
```

Для восстановления:

```
/opt/kaspersky/kuma/mongodb/bin/mongorestore --drop --archive=<путь к архиву>
```

Полезные ссылки

- Резервное копирование KUMA (онлайн-справка):

<https://support.kaspersky.com/help/KUMA/2.1/ru-RU/222208.htm>

- Создание резервной копии Ядра KUMA (Postman): <https://www.postman.com/kl-ru-presales/workspace/kaspersky-products-apis-ru/request/23340929-bd766c26-c34b-467e-a28a-4ff65ac05328>
- Восстановление Ядра KUMA из резервной копии (Postman):
<https://www.postman.com/kl-ru-presales/workspace/kaspersky-products-apis-ru/request/23340929-974b96b4-0876-449c-9001-9912783f6acc>

Revision #19

Created 10 August 2023 13:27:25 by Boris RZR

Updated 19 December 2024 07:21:20 by Boris RZR